

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

**Template Version 1.0, Released on 2017-06-21**



# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 23/05/2018 | 1.0 | Trijeet | Attempt 1 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

**[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In** [**Google Docs**](https://support.google.com/docs/answer/116338?co=GENIE.Platform%3DDesktop&hl=en)**, you can use headings for each section and then go to Insert > Table of Contents.** [**Microsoft Word**](https://support.microsoft.com/en-us/help/285059/how-to-create-a-table-of-contents-by-marking-text-in-word) **has similar capabilities]**

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Purpose of the Technical Safety Concept](#_fulgh8sf1ocg)

[Inputs to the Technical Safety Concept](#_757cx6xm46zb)

[Functional Safety Requirements](#_2f9rjqxbsp2)

[Refined System Architecture from Functional Safety Concept](#_qp3s9pvua9mt)

[Functional overview of architecture elements](#_cqb49updinx4)

[Technical Safety Concept](#_mx8us8onanqo)

[Technical Safety Requirements](#_lnxjuovv6kca)

[Refinement of the System Architecture](#_74udkdvf7nod)

[Allocation of Technical Safety Requirements to Architecture Elements](#_g2lqf7kmbspk)

[Warning and Degradation Concept](#_4w6r8buy4lrp)

# Purpose of the Technical Safety Concept

The purpose of the functional safety concept is to identify the high level system requirements without diving deep into the technical aspects. Different parts of the item architecture are allocated with the responsibility of fulfilling these requirements. The result of this leads to construction of the technical safety requirements from it. Validation and verification instructions for these requirements are also laid down in this. Finally, these requirements will be considered while hardware and software implementation of the system.

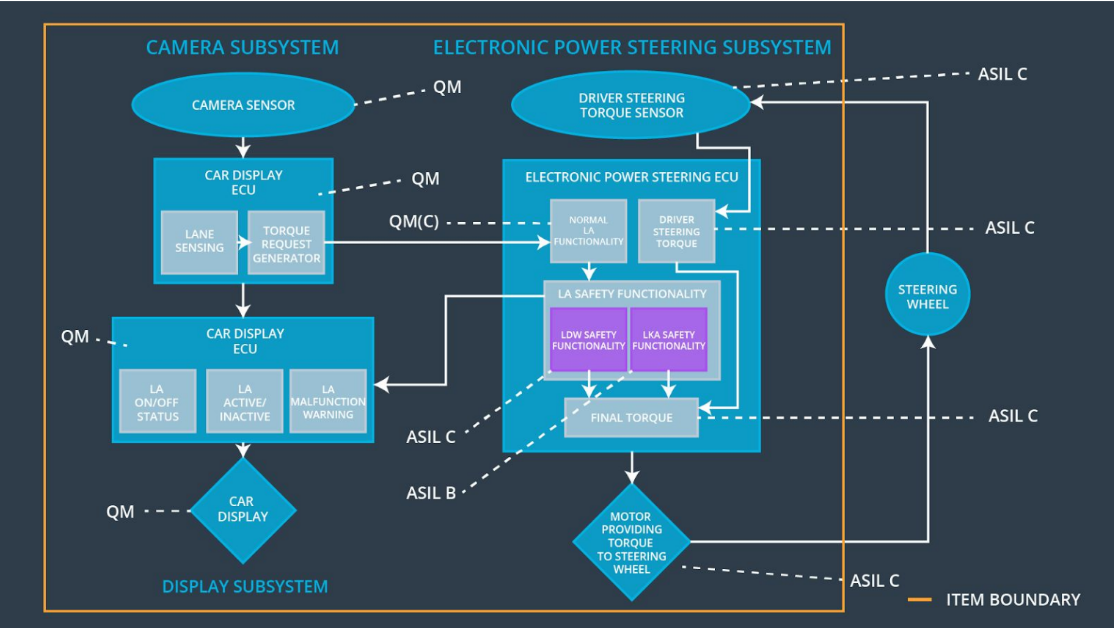
# Inputs to the Technical Safety Concept

## Functional Safety Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | The lane keeping assistance function shall ensure that the lane departure oscillation torque amplitude stays below Max\_Torque\_Amplitude | C | 50 ms | Oscillation torque amplitude maintained below Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | The lane keeping assistance function shall ensure that the lane departure oscillation torque frequency stays below Max\_Torque\_Frequency | C | 50 ms | Oscillation torque amplitude maintained below Max\_Torque\_Frequency |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for no more than Max\_Duration | B | 500 ms | Lane keeping assistance torque is set to 0 |

## Refined System Architecture from Functional Safety Concept

**[Instructions: Provide the refined system architecture from the functional safety concept]**



### 

### Functional overview of architecture elements

**[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item? ]**

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures the scene in front of the car and feeds the image to the camera sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Detects the lane lines in the image from the camera sensor feed. |
| Camera Sensor ECU - Torque request generator | Calculates the amount of torque required and requests the same to the Electronic Power Steering ECU. |
| Car Display | Displays warning notifications. |
| Car Display ECU - Lane Assistance On/Off Status | Indicates whether the lane assistance is turned on or off. |
| Car Display ECU - Lane Assistant Active/Inactive | Indicates whether the lane assistant is currently being used (active) or not (inactive). |
| Car Display ECU - Lane Assistance malfunction warning | Indicates whether the lane assistance system malfunctioned. |
| Driver Steering Torque Sensor | Detects the amount of torque being applied by the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Receives the torque applied by the driver from the Driver Steering Torque Sensor. |
| EPS ECU - Normal Lane Assistance Functionality | Receives the torque request from the Camera Sensor ECU - Torque request generator |
| EPS ECU - Lane Departure Warning Safety Functionality | Ensures that the torque amplitude and frequency are below Max\_Torque\_Amplitude and Max\_Torque\_Frequency respectively. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensures that the torque request is not active for more than Max\_Duration. |
| EPS ECU - Final Torque | Computes the effective torque required by combining the torque request from the lane departure warning and lane keeping assistance functions. |
| Motor | Applies the necessary torque onto the steering wheel. |

# Technical Safety Concept

## Technical Safety Requirements

**[Instructions: Fill in the technical safety requirements for the lane departure warning first functional safety requirement. We have provided the associated functional safety requirement in the first table below. Hint: The technical safety requirements were discussed in the lesson videos. The architecture allocation column should contain element names such as LDW Safety block, Data Transmission Integrity Check, etc. Allocating the technical safety requirements to the "EPS ECU" does not provide enough detail for a technical safety concept.]**

**Lane Departure Warning (LDW) Requirements:**

Functional Safety Requirement 01-01 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-01 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | Lane departure warning safety component shall ensure that the amplitude of the LDW\_Torqie\_Request sent to Final\_EPS\_Torque component is below Max\_Torque\_Amplitude | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to 0 |
| Technical  Safety  Requirement  02 | During any malfunction of LDW function, the function will be disabled and LDW\_Torque\_Request is set to 0 | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to 0 |
| Technical  Safety  Requirement  03 | Once the LDW is disabled, a signal shall be sent to the car display showing a warning notification regarding this. | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to 0 |
| Technical  Safety  Requirement  04 | Correctness of the data sent to the LDW\_Torque\_Request shall be ensured. | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to 0 |
| Technical  Safety  Requirement  05 | Memory has to be tested at startup of the EPS ECU to check for problems in the memory. | A | Ignition cycle | Data Transmission Integrity check | LDW\_Torque\_Request is set to 0 |

**[Instructions: Fill in the technical safety requirements for the lane departure warning second functional safety requirement. We have provided the associated functional safety requirement in the table below. Hint:. Most of the technical safety requirements will be the same. At least one technical safety requirement will have to be slightly modified because we are talking about frequency instead of amplitude. These requirements were not given in the lessons]**

Functional Safety Requirement 01-2 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | Lane departure warning safety component shall ensure that the frequency of the LDW\_Torqie\_Request sent to Final\_EPS\_Torque component is below Max\_Torque\_Frequency | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to 0 |
| Technical  Safety  Requirement  02 | During any malfunction of LDW, the function will be disabled and LDW\_Torque\_Request is set to 0 | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to 0 |
| Technical  Safety  Requirement  03 | Once the LDW is disabled, a signal shall be sent to the car display showing a warning notification regarding this. | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to 0 |
| Technical  Safety  Requirement  04 | Correctness of the data sent to the LDW\_Torque\_Request shall be ensured. | C | 50 ms | LDW Safety | LDW\_Torque\_Request is set to 0 |
| Technical  Safety  Requirement  05 | Memory has to be tested at startup of the EPS ECU to check for problems in the memory. | A | Ignition cycle | Data Transmission Integrity check | LDW\_Torque\_Request is set to 0 |

**Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:**

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

**Lane Keeping Assistance (LKA) Requirements:**

**[Instructions: Fill in the technical safety requirements for the lane keeping assistance functional safety requirement 02-01. We have provided the associated functional safety requirement in the table below. Hint:. You can reuse the technical safety requirements from functional safety requirement 01-01. But you need to change the language because we are now looking at a different system. The ASIL and Fault Tolerant Time Interval are different as well.]**

Functional Safety Requirement 02-1 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

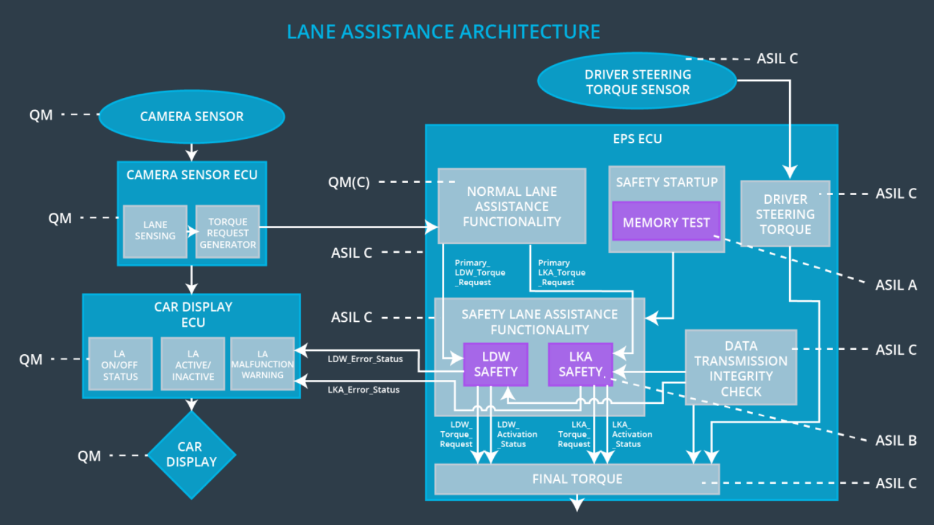
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  01 | Lane keeping assistance safety component shall ensure that the amplitude of the LDW\_Torqie\_Request sent to Final\_EPS\_Torque component is below Max\_Torque\_Amplitude | B | 500 ms | LKA Safety | LKA torque set to 0 |
| Technical  Safety  Requirement  02 | During any malfunction of LDW function, the function will be disabled and LDW\_Torque\_Request is set to 0 | B | 500 ms | LKA Safety | LKA torque set to 0 |
| Technical  Safety  Requirement  03 | Once the LDW is disabled, a signal shall be sent to the car display showing a warning notification regarding this. | B | 500 ms | LKA Safety | LKA torque set to 0 |
| Technical  Safety  Requirement  04 | Correctness of the data sent to the LDW\_Torque\_Request shall be ensured. | B | 500 ms | LKA Safety | LKA torque set to 0 |
| Technical  Safety  Requirement  05 | Memory has to be tested at startup of the EPS ECU to check for problems in the memory. | A | Ignition cycle | Memory check | LKA torque set to 0 |

**Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:**

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

## Refinement of the System Architecture

**[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the technical safety lesson, including all of the ASIL labels.]**



## Allocation of Technical Safety Requirements to Architecture Elements

**[Instructions: We already included the allocation as part of the technical requirement tables. Here you can state that for this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU]**

All technical safety requirements are allocated to the Electronic Power Steering ECU.

## Warning and Degradation Concept

**[Instructions: We've already identified that for any system malfunction, the lane assistance functions will be turned off and the driver will receive a warning light indication. The technical safety requirements have not changed how functionality will be degraded or what the warning will be.**

**So in this case, the warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements. You can copy the functional safety warning and degradation concept here.**

**Oftentimes, a technical safety analysis will lead to a more detailed warning and degradation concept. ]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Disable lane departure warning | Malfunction\_01,  Malfunction\_02 | Yes | Alert on car display: Lane departure warning malfunction |
| WDC-02 | Disable lane keeping assistance | Malfunction\_03 | Yes | Alert on car display: Lane keeping assistance malfunction |